DERWENT-ACC-NO: 1999-434487

DERWENT-WEEK: 199937

TITLE: Database access managing apparatus for e.g. on=line banking - has access managing server that controls database access and detects if user ID accessing database is recorded in user table or access user monitoring table, to confirm user ID and prevent double access

PATENT-ASSIGNEE: SYNTHESIZE KK[SYNTN]

PRIORITY-DATA: 1997JP-0340341 (December 10, 1997)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
JP 11175387 A	July 2, 1999	N/A	011	G06F 012/00

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
JP 11175387A	N/A	1997JP-0340341	December 10, 1997

INT-CL (IPC): G06F012/00, G06F012/14

ABSTRACTED-PUB-NO: JP 11175387A

BASIC-ABSTRACT:

NOVELTY - An access managing server (20) controls the database access and detects if user ID accessing the database is recorded in a user table or an access user monitoring table, to confirm the user ID and prevent double access of the database. DETAILED DESCRIPTION - The database access managing apparatus (1) has a database server (10) that controls a database. A user ID for accessing the database is recorded in a user table. The access data containing the user ID during access of the database are recorded in an access user monitoring table.

USE - For e.g. on-line banking. Also for receiving data e.g. train ticket reservation, plane ticket reservation.

ADVANTAGE - Prevents double access of one user ID to database. Confirms management data during page movement. Ensures reliable transaction processing.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of a database access managing apparatus. (1) Database access managing apparatus; (10) Database server; (20) Access managing server.

CHOSEN-DRAWING: Dwg.1/4

TITLE-TERMS: DATABASE ACCESS MANAGE APPARATUS ON=LINE BANK ACCESS MANAGE SERVE
CONTROL DATABASE ACCESS DETECT USER ID ACCESS DATABASE RECORD USER
TABLE ACCESS USER MONITOR TABLE CONFIRM USER ID PREVENT DOUBLE
ACCESS

DERWENT-CLASS: T01

EPI-CODES: T01-H; T01-H01C2;

SECONDARY-ACC-NO:
Non-CPI Secondary Accession Numbers: N1999-323816

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－175387

(43)公開日　平成11年(1999)７月２日

(51)Int.Cl.⁶		識別記号	FI		
Ｇ０６Ｆ	12/00	５３７	Ｇ０６Ｆ	12/00	５３７Ｄ
	12/14	３２０		12/14	３２０Ａ

審査請求　未請求　請求項の数７　ＯＬ　（全 11 頁）

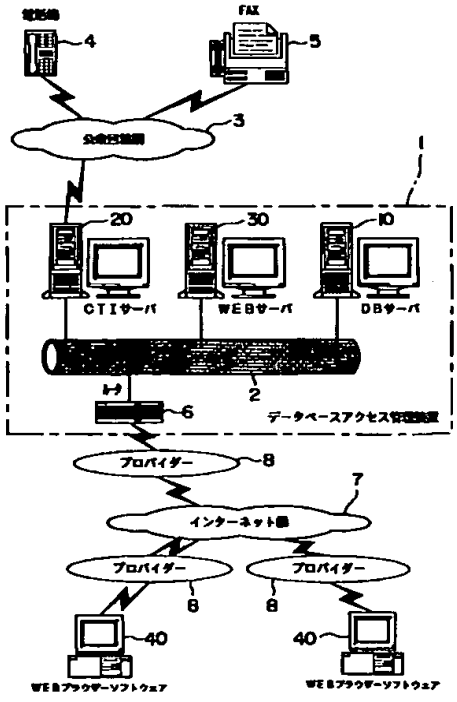
(21)出願番号　特願平9－340341

(22)出願日　平成９年(1997)12月10日

(71)出願人　393026179
株式会社シンセサイズ
東京都江東区東陽５丁目10番５号
(72)発明者　上嶋　靖
東京都江東区東陽５－10－５　株式会社シンセサイズ内
(74)代理人　弁理士　木下　實三　（外１名）

(54)【発明の名称】　データベースアクセス管理装置

(57)【要約】
【課題】　ユーザーの２重アクセスを防止してデータベースサービスを提供できるデータベースアクセス管理装置を提供すること。
【解決手段】　データベースアクセス管理装置１は、データベースを管理するＤＢサーバ１０と、データベースへのアクセスを管理するＣＴＩサーバ２０、ＷＥＢサーバ３０とを備える。ＤＢサーバ１０は、データベースにアクセス可能なユーザーのＩＤ等の情報が記録されたユーザーテーブルと、アクセス中のユーザーのＩＤ等の情報が記録されるアクセスユーザー監視テーブルとを備える。各サーバ１０、２０は、アクセスしてきたユーザーのＩＤがユーザーテーブルに記録されているかを調査してユーザーを確認でき、かつユーザーのＩＤがアクセスユーザー監視テーブルに記録されているかを調査して２重アクセスを防止できる。



1

【特許請求の範囲】

【請求項1】　データベースを管理するデータベース管理手段と、このデータベースへのアクセスを管理するアクセス管理手段とを備え、

前記データベース管理手段には、前記データベースにアクセス可能なユーザーのＩＤを含むユーザー情報が記録されたユーザーテーブルと、データベースにアクセス中のユーザーのＩＤを含むアクセス情報が記録されるアクセスユーザー監視テーブルとが設けられ、

前記アクセス管理手段は、データベースにアクセスしてきたユーザーのＩＤが前記ユーザーテーブルに記録されているか否かを検出してユーザーの確認を行うとともに、前記ユーザーのＩＤがアクセスユーザー監視テーブルに記録されているか否かを検出して２重アクセスを防止する機能を有することを特徴とするデータベースアクセス管理装置。

【請求項2】　請求項1に記載のデータベースアクセス管理装置において、前記アクセス管理手段は、ユーザーがインターネットを利用してデータベースにアクセスする際に用いられるワールドワイドウェブサーバを備え、

前記ユーザーテーブルには、各ユーザーに関してワールドワイドウェブサーバからのアクセス用のＩＤが登録され、かつ前記アクセスユーザー監視テーブルには、前記ＩＤを記録するフィールドが設けられ、

前記アクセス管理手段は、前記ワールドワイドウェブサーバからアクセスしてきたユーザーのＩＤに基づいてユーザーの確認及び２重アクセスのチェックを行うことを特徴とするデータベースアクセス管理装置。

【請求項3】　請求項1に記載のデータベースアクセス管理装置において、前記アクセス管理手段は、ユーザーがインターネットを利用してデータベースにアクセスする際に用いられるワールドワイドウェブサーバと、ユーザーが電話またはＦＡＸを利用してデータベースにアクセスする際に用いられるコンピュータ・テレフォニ・インテグレーションサーバとを備え、

前記ユーザーテーブルには、各ユーザーに関してワールドワイドウェブサーバからのアクセス用のＩＤと、コンピュータ・テレフォニ・インテグレーションサーバからのアクセス用のＩＤとが登録され、かつ前記アクセスユーザー監視テーブルは、前記各ＩＤを個別に記録するフィールドが設けられ、

前記アクセス管理手段は、前記一方のサーバからアクセスしてきたユーザーのＩＤに基づいてユーザーの確認及び２重アクセスのチェックを行った後、アクセスを許可する際に前記アクセスユーザー監視テーブルに他方のサーバ用のＩＤも書き込むように構成されていることを特徴とするデータベースアクセス管理装置。

【請求項4】　請求項2または3に記載のデータベースアクセス管理装置において、前記アクセス管理手段は、前記ワールドワイドウェブサーバからアクセスしてきた

2

際に、そのアクセス時にトランザクション管理データを新たに作成して前記アクセスユーザー監視テーブルに書き込むとともに、前記ワールドワイドウェブサーバを介してユーザーのコンピュータに前記トランザクション管理データを送り、このワールドワイドウェブサーバからのアクセスがあった際には、そのアクセスしてきたユーザーのコンピュータに送られたトランザクション管理データと、前記アクセスユーザー監視テーブルに書き込まれたトランザクション管理データとが一致した場合のみに前記アクセスを許可することを特徴とするデータベースアクセス管理装置。

【請求項5】　請求項4に記載のデータベースアクセス管理装置において、前記アクセス管理手段は、前記ワールドワイドウェブサーバからアクセスしてきた際に、前記トランザクション管理データの他に、ユーザーのＩＰアドレスを前記アクセスユーザー監視テーブルに書き込み、ワールドワイドウェブサーバからのアクセスがあった際には、そのアクセスしてきたユーザーのコンピュータに送られたトランザクション管理データおよびＩＰアドレスと、前記アクセスユーザー監視テーブルに書き込まれたトランザクション管理データおよびＩＰアドレスとが一致した場合のみに前記アクセスを許可することを特徴とするデータベースアクセス管理装置。

【請求項6】　請求項4または5に記載のデータベースアクセス管理装置において、前記トランザクション管理データは、ユーザーが前記ワールドワイドウェブサーバ上の異なるページに移動する度に書き換えられることを特徴とするデータベースアクセス管理装置。

【請求項7】　請求項2～6のいずれかに記載のデータベースアクセス管理装置において、前記アクセス管理手段は、ユーザーが前記ワールドワイドウェブサーバ上の異なるページに移動する度に、前記アクセスユーザー監視テーブルにそのユーザーのページ移動に関する進捗情報を書き込むことを特徴とするデータベースアクセス管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、各種のデータが保管されたデータベースへのアクセスを管理するデータベースアクセス管理装置に関する。

【０００２】

【背景技術】従来より、銀行のオンラインや、電車や飛行機の予約など、各種情報提供サービスを電話やＦＡＸを利用して受けることが行われている。ところで、近年、インターネットの普及により、従来、電話やＦＡＸのみでサービスを行っていた各種データサービスを、ユーザーのパソコンからインターネット網を介して受けられるようにすることが望まれている。

【０００３】このため、電話やＦＡＸ等から公衆回線網を介して接続してくるユーザーに対してＤＢ（データベ

ース）サーバへのアクセスを制御するＣＴＩ（コンピュータ・テレフォニ・インテグレーション）サーバの他に、パソコンからインターネット網を介して接続してくるユーザーに対してＤＢサーバへのアクセスを制御するＷＥＢ（ワールドワイドウェブ）サーバを設けて、これらの各サーバをデータベースへのゲートウェイトして利用することでデータベースサービスを利用できるようにすることが求められていた。

【０００４】

【発明が解決しようとする課題】しかしながら、このような種類の異なるアクセス手段を設けた場合には、１人のユーザーが電話およびパソコンの２種類のアクセス手段を利用してデータベースに接続する２重アクセスが可能となってしまい、特に銀行の残高照会や飛行機等の予約、さらにはユーザーに対してタイムチャージなどで課金するデータベースサービス等の厳密なアクセス制御を行う必要があるサービスを提供することができないという問題がある。

【０００５】また、ＷＥＢサーバは、データ通信の方式としてパケット交換方法を採用しているため、ＷＥＢサーバ上に設けられるアクセス用のページの後に表示されるデータベースサービス用のページのアドレスを知っていると、アクセス用ページを通らずに、データベースサービスを受けることができ、データベースサービスにおけるトランザクション処理、特にサービスの開始および終了の管理を行うことができないという問題もある。

【０００６】本発明の第１の目的は、ユーザーの２重アクセスを防止してデータベースサービスを提供できるデータベースアクセス管理装置を提供することにある。

【０００７】また、本発明の第２の目的は、ＷＥＢサーバを用いた場合に、トランザクション処理を確実に行えるデータベースアクセス管理装置を提供することにある。

【０００８】

【課題を解決するための手段】本発明のデータベースアクセス管理装置は、データベースを管理するデータベース管理手段と、このデータベースへのアクセスを管理するアクセス管理手段とを備え、前記データベース管理手段には、前記データベースにアクセス可能なユーザーのＩＤを含むユーザー情報が記録されたユーザーテーブルと、データベースにアクセス中のユーザーのＩＤを含むアクセス情報が記録されるアクセスユーザー監視テーブルとが設けられ、前記アクセス管理手段は、データベースにアクセスしてきたユーザーのＩＤが前記ユーザーテーブルに記録されているか否かを検出してユーザーの確認を行うとともに、前記ユーザーのＩＤがアクセスユーザー監視テーブルに記録されているか否かを検出して２重アクセスを防止する機能を有することを特徴とする。

【０００９】データベース管理手段に、ユーザーテーブルおよびアクセスユーザー監視テーブルを設け、アクセス管理手段によって、データベースにアクセスしてきたユーザーが、ユーザーテーブルに登録されているか否かのユーザーの確認と、アクセスユーザー監視テーブルに記録されているか否かの２重アクセスのチェックとを行っているので、複数のアクセス手段が設けられている場合でも、２重アクセスを確実に防止できる。

【００１０】この際、前記アクセス管理手段は、ユーザーがインターネットを利用してデータベースにアクセスする際に用いられるワールドワイドウェブサーバ（ＷＥＢサーバ）を備え、前記ユーザーテーブルには、各ユーザーに関してＷＥＢサーバからのアクセス用のＩＤが登録され、かつ前記アクセスユーザー監視テーブルには、前記ＩＤを記録するフィールドが設けられ、前記アクセス管理手段は、前記ＷＥＢサーバからアクセスしてきたユーザーのＩＤに基づいてユーザーの確認及び２重アクセスのチェックを行うことが好ましい。

【００１１】アクセス管理手段に、ＷＥＢサーバを設けた場合でも、ユーザーの確認及び２重アクセスの防止を実現でき、インターネット網を利用したデータベースサービスを行うことができる。

【００１２】また、前記アクセス管理手段は、ユーザーがインターネットを利用してデータベースにアクセスする際に用いられるワールドワイドウェブサーバ（ＷＥＢサーバ）と、ユーザーが電話またはＦＡＸを利用してデータベースにアクセスする際に用いられるコンピュータ・テレフォニ・インテグレーションサーバ（ＣＴＩサーバ）とを備え、前記ユーザーテーブルには、各ユーザーに関してＷＥＢサーバからのアクセス用のＩＤと、ＣＴＩサーバからのアクセス用のＩＤとが登録され、かつ前記アクセスユーザー監視テーブルは、前記各ＩＤを個別に記録するフィールドが設けられ、前記アクセス管理手段は、前記一方のサーバからアクセスしてきたユーザーのＩＤに基づいてユーザーの確認及び２重アクセスのチェックを行った後、アクセスを許可する際に前記アクセスユーザー監視テーブルに他方のサーバ用のＩＤも書き込むように構成されているものでもよい。

【００１３】ＣＴＩサーバとＷＥＢサーバとを設けたので、データベースサービスを、電話やＦＡＸだけでなく、パソコンを利用しても受けることができる。このため、サービスを受けられるユーザーが増え、様々なデータベースサービスを容易に受けることができる。また、ユーザーテーブルおよびアクセスユーザー監視テーブルに記録するＩＤを、各サーバからのアクセス毎に設定しているので、同一ユーザーに対してＣＴＩサーバ用とＷＥＢサーバ用とに異なるＩＤを設定することができ、ＩＤの管理を厳密にできる。

【００１４】さらに、前記アクセス管理手段は、前記ワールドワイドウェブサーバ（ＷＥＢサーバ）からアクセスしてきた際に、そのアクセス時にトランザクション管理データを新たに作成して前記アクセスユーザー監視テ

ーブルに書き込むとともに、前記WEBサーバを介してユーザーのコンピュータに前記トランザクション管理データを送り、このWEBサーバからのアクセスがあった際には、そのアクセスしてきたユーザーのコンピュータに送られたトランザクション管理データと、前記アクセスユーザー監視テーブルに書き込まれたトランザクション管理データとが一致した場合のみに前記アクセスを許可するように構成されていることが好ましい。

【0015】この際、前記アクセス管理手段は、前記トランザクション管理データだけではなく、ワールドワイドウェブサーバを介してアクセスしてきたユーザーのIPアドレスを前記アクセスユーザー監視テーブルに書き込み、ワールドワイドウェブサーバからのアクセスがあった際には、そのアクセスしてきたユーザーのコンピュータに送られたトランザクション管理データおよびIPアドレスと、前記アクセスユーザー監視テーブルに書き込まれたトランザクション管理データおよびIPアドレスとが一致した場合のみに前記アクセスを許可するように構成されていることが好ましい。

【0016】このような本発明では、WEBサーバを介してアクセスするユーザーに対してもアクセス時のトランザクション処理を確実に行うことができる。

【0017】また、前記トランザクション管理データは、ユーザーが前記ワールドワイドウェブサーバ上の異なるページに移動する度に書き換えられることが好ましい。このように構成すれば、ページを移動する度に、ユーザーのコンピュータに送られるとともに、アクセスユーザー監視テーブルに書き込まれるトランザクション管理データの内容を書き換えるため、例えば、どのページまで移動したかなどのサービスの進捗状況を情報として記録することができる。このため、ワールドワイドウェブサーバ上の複数のページを順次移動して情報サービスを行う場合に、1度通過したページには再度戻れないような高度なトランザクション処理を実現することができる。

【0018】さらに、前記アクセス管理手段は、ユーザーが前記ワールドワイドウェブサーバ上の異なるページに移動する度に、前記アクセスユーザー監視テーブルにそのユーザーのページ移動に関する進捗情報を書き込んでもよい。この場合も、ユーザーがどのページまで移動したかなどのサービスの進捗状況をアクセスユーザー監視テーブルに記録できるため、クッキーを用いない場合や書き換えない場合であっても、ユーザーの進捗状況を管理でき、高度なトランザクション処理を実現することができる。

【0019】

【発明の実施の形態】以下、本発明の実施の一形態を図面に基づいて説明する。図1には、本実施形態のデータベースアクセス管理装置1が示されている。データベースアクセス管理装置1は、データベース管理手段であるデータベースサーバ（DBサーバ）10と、アクセス管理手段であるコンピュータ・テレフォニ・インテグレーションサーバ（CTIサーバ）20、および、ワールドワイドウェブサーバ（WEBサーバ）30とを備えている。これらの各サーバ10，20，30は、LAN（ローカルエリアネットワーク）2を介して互いに接続されている。なお、本実施形態では、各サーバ10，20，30は、別々のパソコン（パーソナルコンピュータ）で構成されている。

【0020】DBサーバ10は、図2にも示すように、LAN2に接続するためのネットワークカード11と、このネットワークカード11等の各種のデバイス（周辺機器）を制御するドライバ12と、パソコンを制御管理するOS（オペレーティング・システム）13と、各種データが記録されたデータベーステーブル（DBテーブル）14と、このDBテーブル14を管理するDBエンジン15とを備えている。

【0021】CTIサーバ20は、ネットワークカード21と、公衆回線網3を介した電話機4やFAX5等との接続を制御するCTIボード22と、このネットワークカード21やCTIボード22等の各種のデバイスを制御するドライバ23と、OS24と、電話機4やFAX5等による接続サービスを制御するCTIアプリケーション25と、前記電話機4やFAX5からの入力をDBサーバ10に渡して電話機4等によるデータベースサービスを実現するCTI-DBミドルウェア26とを備えている。

【0022】なお、CTIボード22は、ボード上にDSP（デジタル信号処理専用のマイクロプロセッサ）、CPU、RAM、FlashROM、モデムICなどを搭載して構成されるものであり、FlashROMの書き換えにより、ISDNを用いたデジタル公衆回線網（INS64～INS1500）やアナログ公衆回線網への接続が可能に構成されている。

【0023】WEBサーバ30は、ネットワークカード31と、各種のデバイスを制御するドライバ32と、OS33と、ルータ6、インターネット網7、インターネット網7への接続サービスを行うプロバイダー8等を介して前記LAN2に接続されたパソコン40のWEBブラウザーソフトウェアからのアクセス等を処理するWEBアプリケーション34と、WEBアプリケーション34で管理されかつ各種入力フォーム等がHTML（Hyper Text Markup Language）で記載されたHTML文書35と、アクセスユーザーの管理を行うアクセスユーザー監視アプリケーション36と、パソコン40からの入力をDBサーバ10に渡してインターネットを利用したデータベースサービスを実現するWEB-DBミドルウェア37とを備えている。

【0024】DBサーバ10のDBテーブル14は、図3に示すような、ユーザーテーブル50と、アクセスユ

ーザー監視テーブル６０と、データベースサービス用の各種のデータが蓄積されたデータテーブル７１とを備えている。

【００２５】ユーザーテーブル５０は、データベースサービスを受けるために予め登録されたユーザーの各種データが記録されるものである。具体的には、ユーザーを認識するためのＩＤと、ユーザー名、住所、電話番号等の各種データ５３が記録されている。

【００２６】なお、ＩＤには、ＣＴＩサーバ２０を利用する際に用いられるＣＴＩ－ＩＤ５１と、ＷＥＢサーバ３０を利用する際に用いられるＷＥＢ－ＩＤ５２とが設けられている。これらのＩＤは、共通したものでもよいが、電話等では通常数字しか入力できないためにＣＴＩ－ＩＤ５１も数字のみで構成されるのに対し、ＷＥＢ－ＩＤ５２はパソコン４０を用いるために数字以外に英文字等も利用でき、ユーザー等にとって理解しやすいＩＤを設定できるという利点がある。

【００２７】アクセスユーザー監視テーブル６０は、実際にＤＢサーバ１０にアクセスしているユーザーの情報を管理し、ユーザーの２重アクセスの防止およびトランザクション管理を行うためのものである。具体的には、アクセスしているユーザーのＣＴＩ－ＩＤ６１、ＷＥＢ－ＩＤ６２、アクセス種別６３、ユーザーのパソコン４０に割り当てられたＩＰアドレス６４、トランザクション管理データとして利用されるクッキーの乱数６５、ＣＴＩ－ＤＢミドルウェア２６が最後に使用された時間が記録されるＣＴＩ－ＤＢミドルウェア最終使用ＬＯＧ６６、ＷＥＢ－ＤＢミドルウェア３７が最後に使用された時間が記録されるＷＥＢ－ＤＢミドルウェア最終使用ＬＯＧ６７、ＣＴＩ－ＩＤの有効時間６８、ＷＥＢ－ＩＤの有効時間６９、その他の各種データ７０が記録されるフィールドを備えている。

【００２８】なお、各有効時間６８，６９は、ＣＴＩ－ＤＢミドルウェア２６やＷＥＢ－ＤＢミドルウェア３７が最後に使用された時から有効時間６８，６９に設定された時間が経過した場合には、ユーザーからのアクセスが終了していると判断し、アクセスユーザー監視テーブル６０から各ユーザーのデータを削除するのに利用される。

【００２９】次に、このような本実施形態におけるデータベースアクセス管理の方法について説明する。

【００３０】［ＣＴＩサーバのデータベースアクセス（２重アクセス防止処理）］ユーザーが電話機４やＦＡＸ５を用い、ＣＴＩボード２２に接続された公衆回線網３を介してＣＴＩサーバ２０にアクセスすると、ＣＴＩアプリケーション２５は自動着信、自動応答を行い、ＣＴＩサービスによるＤＢサーバ１０へのアクセスサービスを提供する。

【００３１】具体的には、ＣＴＩアプリケーション２５は、応答メッセージ等によってユーザーに対しアクセス用ＩＤの入力を要求する。この要求に対してユーザーが、ＤＴＭＦ（Dual Tone Multi Frequency,プッシュ信号）、ダイヤルパルス、ＦＡＸ（ＦＡＸ原稿に書かれたＩＤをＣＴＩアプリケーション２５に付加したＯＣＲ機能で認識する）、音声（ＣＴＩアプリケーション２５に付加した音声認識機能により認識する）等によって入力すると、ＣＴＩアプリケーション２５はこのＩＤをＣＴＩ－ＤＢミドルウェア２６に渡す。

【００３２】ＣＴＩ－ＤＢミドルウェア２６は、ＤＢサーバ１０上のＤＢエンジン１５に自動的にログインし、ユーザーの入力したＩＤを元にＳＱＬ文を作成し、ＤＢエンジン１５に検索を依頼する。

【００３３】ＤＢエンジン１５は、ＳＱＬ文に基づきＤＢテーブル１４におけるユーザーテーブル５０を調査し、入力されたＩＤが存在するかをチェックする。この際、ユーザーはＣＴＩサーバ２０を介してアクセスしているため、入力されたＩＤがＣＴＩ－ＩＤ５１に存在するかがチェックされる。なお、ユーザーテーブル５０にＣＴＩ－ＩＤ５１の有効・無効のフラグや、その他の条件フィールドがある場合には、それらも合わせてチェックする。

【００３４】ＤＢエンジン１５は、ユーザーテーブル５０を調査した結果をＳＱＬ文にてＣＴＩ－ＤＢミドルウェア２６に返す。ＣＴＩ－ＤＢミドルウェア２６は、ＳＱＬ文を解釈してＣＴＩアプリケーション２５に結果を渡す。

【００３５】ユーザーテーブル５０の調査結果が無効、つまり該当するＩＤが存在しない場合や、無効フラグが設定されていたり、その他の条件がクリアされていない場合には、ユーザーはＣＴＩサーバ２０を介してデータベースサービスを受けることができない。なお、この調査結果は、ＣＴＩアプリケーション２５の機能により、ユーザーの電話機４やＦＡＸ５に返すことができる。

【００３６】一方、ユーザーテーブル５０の調査結果が有効の場合には、ＣＴＩアプリケーション２５はＣＴＩ－ＤＢミドルウェア２６に、アクセスユーザー監視テーブル６０に同一のＩＤが無いか調査を依頼する。ＣＴＩ－ＤＢミドルウェア２６は、ＳＱＬ文を発行してＤＢエンジン１５に渡し、入力されたＩＤがアクセスユーザー監視テーブル６０のＣＴＩ－ＩＤ６１にあるかをチェックする。

【００３７】ここで、同一のＩＤが監視テーブル６０にある場合には、ＣＴＩアプリケーション２５は、既に同一ユーザーがアクセス中と判断し、アクセスを許可しない。一方、同一のＩＤが監視テーブル６０に無い場合には、その入力されたＩＤを監視テーブル６０のＣＴＩ－ＩＤ６１に書き込み、データテーブル７１へのアクセスを許可する。

【００３８】なお、本実施形態では、各ユーザーに対してＣＴＩ－ＩＤ５１およびＷＥＢ－ＩＤ５２の２種類の

ＩＤを設定しているため、ＣＴＩアプリケーション２５はＣＴＩ－ＤＢミドルウェア２６を介してユーザーテーブル５０を調査し、アクセス条件が有効と判断した際に、ＷＥＢ－ＩＤ５２の情報もユーザーテーブル５０より入手する。そして、ＣＴＩアプリケーション２５がＣＴＩ－ＤＢミドルウェア２６を通じてＣＴＩ－ＩＤをアクセスユーザー監視テーブル６０に書き込む際に、ＷＥＢ－ＩＤ５２も監視テーブル６０のＷＥＢ－ＩＤ６２に同時に書き込み、さらに、アクセス種別６３にＣＴＩサーバ２０を介したアクセスであることを表すフラグを立てる。

【００３９】その後、ユーザーは、ＣＴＩアプリケーション２５の音声案内に従い、ＣＴＩサービスを受けることができるとともに、ＣＴＩサーバ２０をゲートウェイとしてデータベースサービスを受けることができる。また、データベースの出力は、ＣＴＩアプリケーション２５の機能を利用して音声やＦＡＸによって出力できる。すなわち、データベースへの入力及び出力は、ＣＴＩアプリケーション２５の機能によって操作できる。

【００４０】ＣＴＩサーバ２０上のユーザーサービスの終了は、ユーザーが回線を切断すれば必ずその回線切断信号が上がってくるという特性を利用している。つまり、ＣＴＩアプリケーション２５は、回線切断信号を受け取ったら、ＣＴＩ－ＤＢミドルウェア２６を通じてアクセスユーザー監視テーブル６０に書き込んだＩＤを消去し、ＤＢエンジン１５よりログアウトする。

【００４１】但し、何らかの原因で、電話回線から切断信号が上がってこない可能性もある。この場合、アクセスユーザー監視テーブル６０にＩＤが書き込まれたままであるため、そのユーザーはＣＴＩサーバ２０およびＷＥＢサーバ３０のいずれからもアクセスできなくなる。このため、本実施形態では、ＣＴＩ－ＤＢミドルウェア２６は、ＤＢエンジン１５にリクエストを出す度に、アクセスユーザー監視テーブル６０のＣＴＩ－ＤＢミドルウェア最終使用ＬＯＧ６６に時間を書き込むようにしている。

【００４２】そして、ＣＴＩアプリケーション２５は、ＣＴＩ－ＤＢミドルウェア２６を通じてアクセスユーザー監視テーブル６０の中で、アクセス種別６３がＣＴＩでありかつＣＴＩ－ＤＢミドルウェア最終使用ＬＯＧ６６に書き込まれた最終使用時間からＣＴＩ－ＩＤの有効時間６８に設定された時間が経過したデータを消去する。なお、ＣＴＩアプリケーション２５は、電話機４やＦＡＸ５からの接続の有無に関わらず作動できるため、有効時間を過ぎたデータ消去の処理は、一定時間間隔で行うようにすればよい。

【００４３】〔ＣＴＩサーバ２０のトランザクション処理〕ＣＴＩサーバ２０は、公衆回線網３を経由してＣＴＩアプリケーション２５が応答する回線交換サービスなので、ＣＴＩアプリケーション２５の応答からサービスの終了までは、１つのトランザクションとして容易に管理できる。

【００４４】［ＷＥＢサーバのデータベースアクセス（２重アクセス防止処理）］パソコン４０等のクライアントＰＣや、ワークステーション、モバイル端末機上で動作するＷＥＢブラウザーソフトウェアによって、ＤＢサーバ１０にアクセスする場合には、ユーザーは、インターネット網７やその他のＷＡＮ（ワイドエリアネットワーク）を経由してＷＥＢサーバ３０に接続する。なお、ユーザーのクライアントＰＣは、プロバイダー８と呼ばれるインターネットへの接続サービスを行う企業を介して、ダイヤルアップあるいは専用線接続により、ＴＣＰ／ＩＰプロトコルを用いてインターネット網７に接続される。

【００４５】ユーザーは、ＷＥＢブラウザーソフトウェアを用い、ＨＴＭＬ文書３５上のＤＢサーバ１０へのアクセス用ＩＤの入力フォームにＩＤを入力する。このフォームに入力されたＩＤは、アクセスユーザー監視アプリケーション３６を経由し、ＷＥＢ－ＤＢミドルウェア３７に渡される。

【００４６】ＷＥＢ－ＤＢミドルウェア３７は、ＤＢサーバ１０上のＤＢエンジン１５に自動的にログインし、ユーザーの入力したＩＤを元にＳＱＬ文を作成し、ＤＢテーブル１４のユーザーテーブル５０に入力されたＩＤが存在するかをチェックする。この際、ユーザーはＷＥＢサーバ３０を介してアクセスしているため、入力されたＩＤがＷＥＢ－ＩＤ５２に存在するかがチェックされる。なお、ユーザーテーブル５０にＷＥＢ－ＩＤ５２の有効・無効のフラグや、その他の条件フィールドがある場合には、それらも合わせてチェックする。

【００４７】ＤＢエンジン１５は、ユーザーテーブル５０を調査した結果をＳＱＬ文にてＷＥＢ－ＤＢミドルウェア３７に返す。ＷＥＢ－ＤＢミドルウェア３７は、ＳＱＬ文を解釈してアクセスユーザー監視アプリケーション３６に結果を渡す。

【００４８】ユーザーテーブル５０の調査結果が無効、つまり該当するＩＤが存在しない場合や、無効フラグが設定されていたり、その他の条件がクリアされていない場合には、ユーザーはＷＥＢサーバ３０を介してデータベースサービスを受けることができない。

【００４９】一方、ユーザーテーブル５０の調査結果が有効の場合には、アクセスユーザー監視アプリケーション３６は、ＷＥＢ－ＤＢミドルウェア３７に、アクセスユーザー監視テーブル６０に同一のＩＤが無いか調査を依頼する。ＷＥＢ－ＤＢミドルウェア３７は、ＳＱＬ文を発行してＤＢエンジン１５に渡し、入力されたＩＤがアクセスユーザー監視テーブル６０のＷＥＢ－ＩＤ６２にあるか否かをチェックする。

【００５０】ここで、同一のＩＤが監視テーブル６０にある場合には、アクセスユーザー監視アプリケーション

３６は、既に同一ユーザーがアクセス中と判断し、アクセスを許可しない。一方、同一のＩＤが監視テーブル６０に無い場合には、そのＩＤおよびユーザーテーブル５０から読みとったそのユーザーのＣＴＩ－ＩＤ５１を監視テーブル６０のＷＥＢ－ＩＤ５２およびＣＴＩ－ＩＤ５１に書き込むとともに、アクセス種別６３にＷＥＢサーバ３０を介したアクセスであることを表すフラグを立てる。さらに、アクセスユーザー監視アプリケーション３６は、ユーザーのパソコン４０のＩＰアドレスを入手し、監視テーブル６０のＩＰアドレス６４に書き込み、データテーブル７１へのアクセスを許可する。

【００５１】また、アクセスユーザー監視アプリケーション３６は、英数字等からなる乱数を発行し、クッキー（cookie：ＷＥＢサーバ３０とＷＥＢブラウザーソフトウェアとの間でやり取りされるテキストデータであり、桁数や英数字等のデータ内容は自由に設定できる）に梱包する。そして、このクッキーを、クライアント（パソコン４０）に送るとともに、ＷＥＢ－ＤＢミドルウェア３７を通じて監視テーブル６０のクッキーの乱数フィールド６５に格納する。

【００５２】なお、ＤＢサーバ１０へのアクセスの成功及び失敗は、アクセスユーザー監視アプリケーション３６およびＷＥＢアプリケーション３４を通じてＨＴＭＬ文書３５によってユーザーに伝えることができる。

【００５３】その後、ユーザーは、ＨＴＭＬ文書３５に従ってＷＥＢサービスを受けることができる。また、ＷＥＢサーバ３０をゲートウェイとしてデータベースサービスを受けることができる。この際、データベースの出力は、ＷＥＢアプリケーション３４の機能を利用してＨＴＭＬ文書３５によって出力できる。すなわち、データベースへの入力及び出力は、ＷＥＢアプリケーション３４の機能によって操作できる。

【００５４】データベースからのログアウトは、ＨＴＭＬ文書３５による画面に表示されるログアウトボタンをユーザーがクリックすることにより行う。

【００５５】〔ＷＥＢサーバ３０のトランザクション処理〕ＷＥＢサーバ３０はＣＴＩサーバ２０と異なり、ＴＣＰ／ＩＰパケットによるサービスなので、ＨＴＭＬ文書３５のアクセス用の入力フォームでアクセスした後も、ページ間の移動を管理する必要がある。すなわち、ページ間の移動を管理しなければ、通常、入力フォームでアクセスが許可された以降に表示されるサービスページのアドレスを、ユーザーがブラウザーにダイレクトに入力すると、前記サービスページが表示されてしまう。このため、ログインを行わずにＷＥＢサービスを受けることができてしまい、トランザクションを正確に管理できなくなってしまう。銀行オンライン等の高度なＤＢサービスの提供には、トランザクション処理は必要であるが、ＷＥＢサーバ３０を用いた場合にはパケット交換であるがゆえに、サービスの開始と終了の管理がＷＥＢサーバ３０上では非常に難しいという問題がある。

【００５６】そこで、本実施形態では、前記ＩＰアドレス６４とクッキーを利用してトランザクション処理を実現している。すなわち、ＷＥＢサーバ３０のトランザクションの開始は、前述の２重アクセス防止用のアクセスサービス（ＩＤ入力処理）によって明確に管理できる。

【００５７】アクセスを許可されたアクセス中のユーザーは、アクセスユーザー監視テーブル６０に記録されたＩＰアドレス６４と、クッキーの乱数６５とを持っている。ＩＰアドレス６４は、ユーザーのＴＣＰ／ＩＰ通信で現在利用しているＩＰアドレスであり、またクッキーは１つのログイン毎に（ＩＤ入力処理を行う度）に発行されるため、ユーザーがページを移動する際に、アクセスユーザー監視アプリケーション３６がアクセスしているユーザーのＩＰアドレスおよびクッキーのデータと、アクセスユーザー監視テーブル６０に記録されているＩＰアドレス６４およびクッキーの乱数６５とが一致しているか否かを確認することで、トランザクションを実現できる。

【００５８】すなわち、ユーザーがログインページ（ＩＤ入力ページ）をとばしてダイレクトにサービスページのアドレスを指定しても、アクセスユーザー監視アプリケーション３６がページの移動の度に、ユーザーのクッキーを調査し、アクセスユーザー監視テーブル６０にあるクッキーと比較するため、ログインページをとばして最新のクッキーが与えられていないユーザーはサービスを受けることができなくなり、これにより確実なトランザクション処理を行うことができる。

【００５９】なお、トランザクションサービスの中で、高度な制御をする場合には、アクセスユーザー監視アプリケーション３６は、クッキーの乱数をページ移動の度に書き換えるように構成すればよい。この場合、クッキー内にサービスの進捗状況を記録することもできる。高度なトランザクション処理を必要とするサービス、例えば、１回のログインでデータの書き換えを１度しか許可しないサービスや、ＩＤ自体が１回しか利用できないゲーム参加用のＩＤを用いたサービスを行う場合には、ＩＰアドレスと１回のログインで発行されるクッキーだけで管理すると、ブラウザーのバックボタンを押すと元のページに戻って再度データを入力できたり、ゲームを再度行うことができてしまう。

【００６０】これに対し、ページ移動の度にクッキーを書き換えていけば、例えば乱数データに加えて各ページに対応した情報を組み込むことなどで、ユーザーがどのページまで進んでいるかの進捗状況を管理でき、高度なトランザクションサービスを実現できる。なお、サービスの進捗情報は、ページ間の移動の度に、アクセスユーザー監視アプリケーション３６によってアクセスユーザー監視テーブル６０に記録することで管理してもよい。さらには、クッキーおよびアクセスユーザー監視テーブ

ル60の両方に記録してもよい。

【0061】また、トランザクションの終了は、通常は、前述の通り、ユーザーが画面に表示されるログアウトボタンをクリックすることにより行うが、例えば、ユーザーがダイヤルアップPPP（Point to Point Protocol）接続などでログインしている際に回線が突然切断された場合などの異常終了の場合や、ログインしたユーザーがDBサービスを受けた後にログアウトせずに他のサイトへ移動してしまったり、そのまま放置してしまった場合には、ログアウトが正常に行えず、アクセスユーザー監視テーブル60のデータを消去することができない。このため、異常終了等に応じてユーザーが再度アクセスしようとしても、アクセスユーザー監視テーブル60にIDが残っているため、CTIサーバ20経由でも、WEBサーバ30経由でもアクセスできなくなってしまう。

【0062】このため、ログアウトボタンを押せない場合のために、アクセスユーザー監視アプリケーション36は、アクセスユーザー監視テーブル60に格納されているアクセス中のWEB-ID62とIPアドレス64に対して、設定された間隔でPING（TCP/IPネットワークでIPパケットが通信先まで届いているかどうかや，IP的に到達可能かどうかを調べるコマンド）を実行する。そして、設定された数だけ連続してPINGの応答がない場合には、切断されたと判断し、アクセスユーザー監視アプリケーション36はアクセスユーザー監視テーブル60からそのユーザーのIDを消去する。

【0063】ただし、専用線環境からアクセスしているユーザーや、PPP接続の場合であっても他のWEBサーバに移動しているユーザーの場合には、アクセスユーザー監視アプリケーション36のPINGによる監視にも応答してしまう。その場合、アクセスユーザー監視アプリケーション36は、アクセスユーザー監視テーブル60上のWEB-DBミドルウェア最終使用LOG67と有効時間69をチェックし、最終アクセスLOGからID有効時間を過ぎたユーザーIDをアクセスユーザー監視テーブル60から消去する。

【0064】なお、近年、ダイヤルアップルータやファイヤーウォールでは、1つのグローバルIPアドレスに対して複数のプライベートアドレスを割り振り、LAN等で接続された複数の端末からインターネットを利用できるようになっている。この場合には、アクセスしてきたユーザーとは別のユーザーが他のWEBサーバを利用している場合には、PINGにも応答してしまう。このため、一般ユーザーを対象にしたデータベースサービスを行う場合には、前記有効時間を用いたトランザクションの終了処理を必ず行うようにすればよい。

【0065】また、同一グローバルIPアドレスに複数のプライベートアドレスを割り振って利用している形態のユーザーが、アクセス中にクッキーをコピーし、同一グローバルIPアドレスを利用している他のユーザーのクライアントPCにコピーしてアクセスすると、アクセスユーザー監視アプリケーション36がチェックするのはIPアドレスとクッキーであるから、両方のユーザーがアクセスできてしまう。この場合でも、前述のように、ページ間移動毎にクッキーを書き換える等して進捗管理を行えば、両ユーザーが同一IPアドレスとクッキーとを持っていても、一方のユーザーがページ間移動してしまえばクッキーの内容が書き換えられたり、アクセスユーザー監視テーブル60に進捗情報が記録されるため、一方のユーザーしかサービスを受けられないようにできる。このように進捗を管理することで、重要なサービスはどちらか一方しか受けられない為、仮にクッキーをコピーしてアクセスしようとするユーザーが存在する場合でも、2重ログイン防止とトランザクション管理を実現できる。

【0066】このような本実施形態によれば、次のような効果がある。

①CTIサーバ20およびWEBサーバ30の2種類のアクセス手段を介してDBサーバ10にアクセスしてデータベースサービスを受けることができるため、データベースサービスを、電話機4やFAX5だけでなく、パソコン40を利用しても受けることができる。このため、サービスを受けられるユーザーが増え、様々なデータベースサービスを容易に受けることができる。

【0067】②ユーザーテーブル50およびアクセスユーザー監視テーブル60に記録するIDを、各サーバ20，30に対応して設定しているので、同一ユーザーに対してCTIサーバ20用とWEBサーバ30用とに異なるIDを設定することができる。このため、通常数字のみで構成されるCTI-ID51とは別に、WEB-ID52としては英文字等も利用でき、ユーザー等にとって理解しやすいIDを設定できる。

【0068】③DBサーバ10に、ユーザーテーブル50およびアクセスユーザー監視テーブル60を設け、CTIサーバ20やWEBサーバ30を介してDBサーバ10にアクセスしてきたユーザーが、ユーザーテーブル50に登録されているか否かのユーザー確認と、アクセスユーザー監視テーブル60に記録されているか否かの2重アクセスのチェックとを行っているので、複数のアクセス用サーバ20，30が設けられている場合でも、2重アクセスを確実に防止できる。

【0069】④WEBサーバ30を介したデータベースサービス時に、ユーザーのパソコン40に対してクッキーを送るとともに、そのユーザーのIPアドレスを取得することで、トランザクション処理が困難であるパケット交換によるWEBサービスにおいても、トランザクション処理を実現することができる。

【0070】⑤従って、本実施形態のデータベースアクセス管理装置1では、2重アクセスを確実に防止でき、

かつトランザクション処理を実現できるため、銀行の残高照会等の高度なデータベースサービスを、WEBサービスやCTIサービスにより実現することができる。特に、WEBサービスは、ユーザーにとって運用コストが低いため、データベースサービスを安価に実現することができる。

【0071】なお、本発明は前記実施形態に限定されるものではなく、本発明の目的を達成できる範囲内での変形等は本発明に含まれるものである。

【0072】例えば、前記実施形態では、CTIサーバ20およびWEBサーバ30は、DBサーバ10と同一のLAN2上に設けられていたが、図4に示すように、プロバイダー8およびインターネット網7またはその他のWAN網（フレームリレーやATM網等）を介して前記LAN2に接続された他のLAN80上、つまりDBサーバ10とは別のLAN80上に設けてもよい。

【0073】また、WEBサーバ30を介してデータベースサービスを受けるパソコン40は、LAN2上に設けられていてもよい。この場合、イントラネットと呼ばれる環境となり、特に企業内等でLAN2に接続されたパソコン40を利用して、その会社内に設けられたDBサーバ10にアクセスすることができ、この場合クライアントにはWEBブラウザーソフトウェアのみを用意すればよいため、コストを低減できる。

【0074】前記実施形態では、CTI-ID51およびWEB-ID52の2種類のIDを設定していたが、これらを同一のIDとし、ユーザーテーブル50やアクセスユーザー監視テーブル60にもCTI-ID51、WEB-ID52をまとめて1つのIDとし、CTI-ID61、WEB-ID62をまとめて1つのIDとしてもよい。

【0075】この場合には、先にアクセスユーザー監視テーブル60に入力されたIDがあるかをチェックしてから、ユーザーテーブル50を調査するようにしてもよい。すなわち、2重アクセスのチェックを行い、そこで、同一IDが存在しない場合のみ、ユーザーテーブル50によってユーザーの確認を行うことができるため、全てのユーザーがユーザーテーブル50にアクセスする必要が無くなり、データのトラフィックを減らすことができる。なお、この場合には、アクセスユーザー監視テーブル60に該当するIDが無く、かつユーザーテーブル50におけるアクセス条件が合致した場合にアクセスが許可される。また、アクセスユーザー監視テーブル60へのIDの書き込みは、通常ユーザーテーブル50での確認が終了してからであるが、例えば、あるIDのユーザーがユーザーテーブル50での確認中に他のユーザーが同一IDでアクセスしてくる可能性を考慮し、アクセスユーザー監視テーブル60にIDが無い場合にはその場でIDを書き込み、その後、ユーザーテーブル50での条件を満たさずアクセスを許可されなかった場合のみ、監視テーブル60に書き込まれたIDを消去するようにしてもよい。

【0076】CTI-ID51やWEB-ID52の桁数や、使用する文字、数字の種類などは任意に設定できる。また、ID以外にパスワードの入力を要求するように設計した場合も、同様の手法を用いればよい。

【0077】前記CTI-IDの有効時間68やWEB-IDの有効時間69を利用したログアウト処理は、CTIアプリケーション25やアクセスユーザー監視アプリケーション36以外の、例えばDBサーバ10上の別アプリケーションあるいはLAN2やインターネット網7に接続されたクライアントPC（パソコン40）が行ってもよい。

【0078】また、データベースアクセス管理装置1としては、CTIサーバ20のみを設けてもよいし、WEBサーバ30のみを設けてもよく、これらは提供するデータベースサービスのユーザー等に応じて適宜設定すればよい。

【0079】さらに、前記実施形態では、WEBサーバ30を利用したデータベースサービスにおけるトランザクション処理を実現するために、IPアドレスおよびクッキーを用いていたが、例えば、サービスを受けるパソコン40がイントラネット上に配置されている場合のように、すべてのパソコン40のIPアドレスが一意に設定されている場合には、クッキーを用いずに、ページ間の移動時にIDおよびIPアドレスを確認することによってトランザクション処理を実現してもよい。

【0080】また、ユーザーがページ間を移動する度にクッキーを書き換えるように構成した場合には、IPアドレスをチェックしなくても、トランザクション処理を実現することができる。

【0081】さらに、前記実施形態では、各サーバ10，20，30は、それぞれ別々のコンピュータによって構成されていたが、CTIボード22や、DBエンジン15、CTIアプリケーション25、WEBアプリケーション34等の各アプリケーション等を1つあるいは2つのコンピュータに組み込むことで、各サーバの機能を1つあるいは2つのコンピュータで実現してもよい。

【0082】

【発明の効果】前述のように本発明のデータベースアクセス管理装置によれば、アクセスユーザー監視テーブルを設けているので、ユーザーの2重アクセスを防止したデータベースサービスを提供することができる。

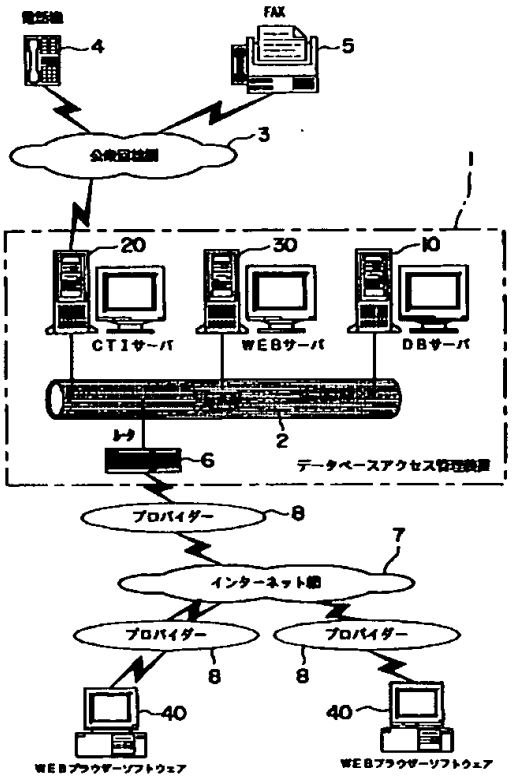
【0083】また、WEBサーバを用いた場合に、トランザクション管理データをクライアントのパソコンに書き込み、ページ間の移動時にその管理データを確認すれば、WEBサーバを用いたデータベースサービスにおいてもトランザクション処理を確実に行うことができる。

【図面の簡単な説明】

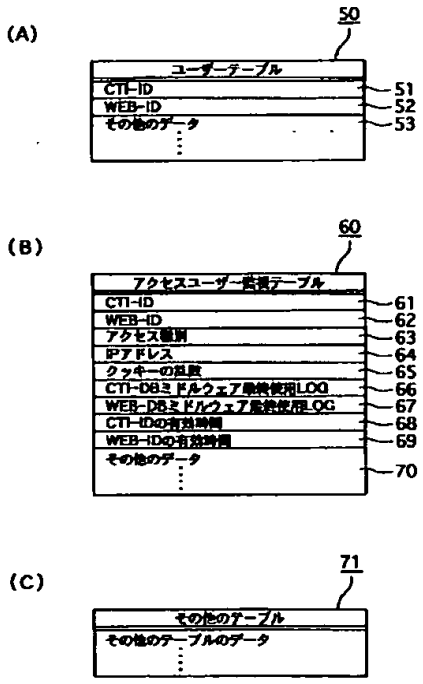
【図1】本発明の一実施形態に係るデータベースアクセ

ス管理装置の構成を示す図である。
【図2】前記実施形態におけるシステム構成を示す図である。
【図3】前記実施形態におけるデータベーステーブルの構成を示す図である。
【図4】本発明の変形例に係るデータベースアクセス管理装置の構成を示す図である。
【符号の説明】
1　データベースアクセス管理装置
2，80　LAN
3　公衆回線網
4　電話機
5　FAX
6　ルータ
7　インターネット網
8　プロバイダー
10　DBサーバ
14　DBテーブル
15　DBエンジン
20　CTIサーバ
22　CTIボード
25　CTIアプリケーション
26　CTI-DBミドルウェア
30　WEBサーバ
34　WEBアプリケーション
35　HTML文書
36　アクセスユーザー監視アプリケーション
37　WEB-DBミドルウェア
40　パソコン
50　ユーザーテーブル
51，61　CTI-ID
52，62　WEB-ID
60　アクセスユーザー監視テーブル
63　アクセス種別
64　IPアドレス
65　クッキーの乱数
66　CTI-DBミドルウェア最終使用LOG
67　WEB-DBミドルウェア最終使用LOG
68　CTI-IDの有効時間
69　WEB-DBの有効時間
71　データテーブル

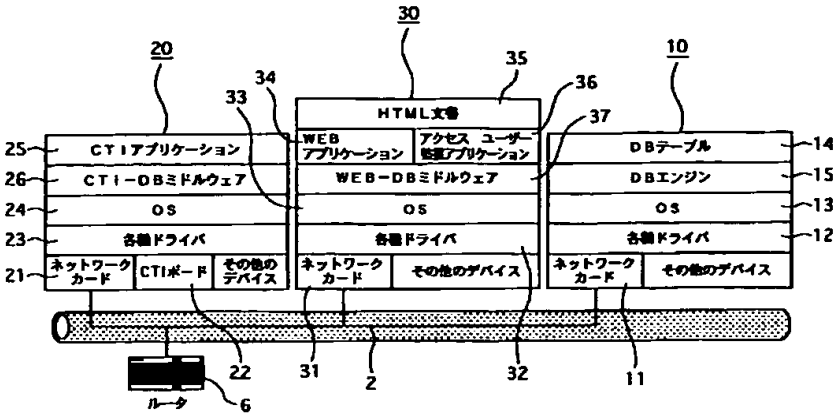
【図1】



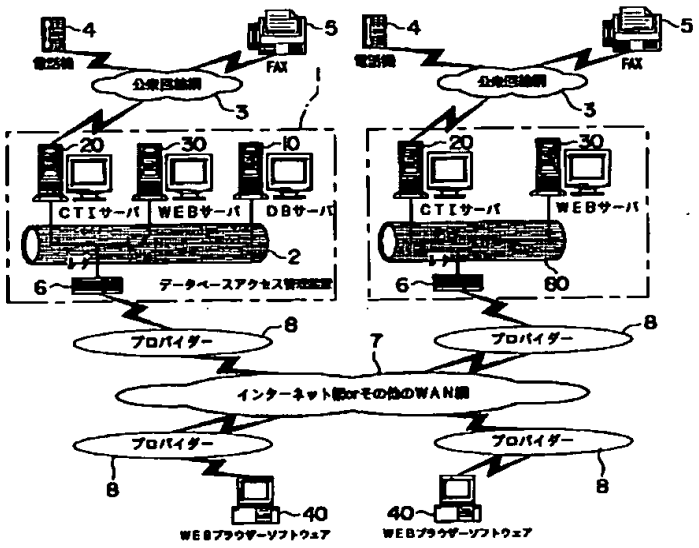
【図3】



【図2】


30
20
10
34
35
36
33
37
HTML文書
WEB アプリケーション
アクセス ユーザー 処理アプリケーション
CTIアプリケーション
DBテーブル
14
25
CTI-DBミドルウェア
WEB-DBミドルウェア
DBエンジン
15
26
OS
OS
OS
13
24
各種ドライバ
各種ドライバ
各種ドライバ
12
23
ネットワークカード
CTIボード
その他のデバイス
ネットワークカード
その他のデバイス
ネットワークカード
その他のデバイス
21
22
31
2
32
11
ルータ
6

【図4】


4
5
電話機
FAX
公衆回線網
3
20
30
10
CTIサーバ
WEBサーバ
DBサーバ
2
6
データベースアクセス管理装置
8
プロバイダー
7
インターネット網orその他のWAN網
40
WEBブラウザーソフトウェア
60